UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/003,847	10/31/2001	Sanguthevar Rajasekaran	020967-001100US	6387

20350 7590 04/21/2004

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
CAPUTO, LISA M	
ART UNIT	**PAPER NUMBER**
2876	

DATE MAILED: 04/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/003,847	RAJASEKARAN ET AL.	
	Examiner	Art Unit	
	Lisa M Caputo	2876	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 January 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Amendment

1. Receipt is acknowledged of the amendment filed 2 January 2004.

Claim Rejections - 35 USC § 102

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-5 are rejected under 35 U.S.C. 102(e) as being anticipated by Vanstone et al. (U.S. Patent No. 6,490,682, from hereinafter "Vanstone").

Vanstone teaches a log-on verification protocol having all of the elements and means as recited in claims 1-5 of the instant application. Regarding claim 1, Vanstone teaches a method of authenticating a client to a server which comprises generating and signing a challenge at the client, and sending the signed challenge to the server (the client sends a request 104 containing the client identification and signature, among other entities, to the server 18 as shown in Figure 2, col 2, lines 52-62), the signature of the challenge is verified at the server (the server then checks that root certifying authority public key is correct 112; the client public key is extracted from the certificate or a lookup 113; is performed on the server database, and the signature s is then verified 114 using the client public key as shown in Figure 2, col 2, lines 63-67), and if the signature is verified, an indication of successful authentication is sent to the client (a response 122 is sent to the client and includes the log-on applet, a signature s', and server's certificate, as shown in Figure 2, col 3, lines 1-13).

Vanstone discloses that the server includes log-on applets, crypto software and other applets. The server also includes a private key PR.sub.S and a certificate CERT.sub.S which includes its public key PU.sub.S. Optionally the server may also include a database of client public keys indexed by a client identification. Referring now to FIG. 2, when the client 12 wishes to request an applet from a server for the first time, the client first authenticates the server by generating a random number x 100, preferably on the hardware token 14 (as recited in claim 2 of the instant application). A counter or a time stamp or the like may generate the value x. A hash H on the concatenation of the client identification ID.sub.C, the root public key and x is computed 102. A signature s of the hash H is calculated using the client private key PR.sub.C 103. The client then sends a request 104 containing ID.sub.C, PU.sub.CA, x, s to the server 18 (as recited in claim 3 of the instant application). The client to indicate the currency of the transaction of session uses the value x. The server then checks that root certifying authority public key PU.sub.CA is correct 112. The client public key PU.sub.C is either extracted 113 from the certificate or a lookup 113' is performed in the server database. The signature s is then verified 114 using PU.sub.C. The server then generates a random number y 116 and computes the hash H' 118 on the concatenated message of the log of the applet, x, y and ID.sub.C. A signature s' on the hash H' is computed using the server private key PR.sub.S 120. A response 122 is sent to the client and includes the log-on applet, y, s' and the server's certificate CERT.sub.S.

Once the client receives this information it verifies the validity of CERT.sub.S 124. The client also verifies x 125, which was sent back with the message from the

server and thus indicating the currency of the session (as recited in claims 4-5 of the instant application). The public key of the server PU.sub.S is extracted from the certificate 126 and used to verify the signature s' 127. This then verifies the server to the client. The value y is also extracted saved by the client 129 to be used in later transactions. Turning to FIG. 3, once the client has verified the server it may then request an appropriate applet by first generating a random number z 210. A request 214 is then sent to the server which includes an identification of the appropriate applet 212 and the random number z. The server then computes a hash H" on the concatenation of the applet, y, z and DC.sub.C 126. The server then computes a signature s" 218 on the hash H" using the private key of the server PR.sub.C. Both the applet and the signature s" are then sent to the client 220. The client verifies the signature 222 using the server public key and once verified may safely use the applet. The value y is also verified 223 to establish currency of the sessio. The value Z is also checked 224 to make sure it is current. If the client requires more applets, steps 210 and 224 are repeated for a given session. When a new session is resumed the client may re-authenticate the server as set out in FIG. 2 (see Figures 1-2, col 2, line 47 to col 3 line 30).

3. Claims 6-8 are rejected under 35 U.S.C. 102(e) as being anticipated by Fite et al. (U.S. Patent No. 6,467,684, from hereinafter "Fite").

Fite teaches a pre-paid card system for purchasing products or services having all of the elements and means as recited in claims 6-8. Regarding claim 6, Fite teaches a method of using a one-time use card number for an online transaction comprising, generating a one-time use card number at a user system (customer internet access

terminal 18); authenticating the user system to an issuer system (host database 12 and card vendor terminal 14); passing the one-time use card number from the user system to the issuer system; passing the one-time use card number from the user system to a merchant system (merchant station 16) where the merchant system presents the one-time use card number to the issuer system to effect a payment; verifying the one-time use card number received from the merchant system with the one-time use card number received from the user system, and if the one-time use card number is verified, approving the transaction (see Figures 1 and 5, col 2 line 60 to col 5 line 30).

Fite discloses that the card vendor terminal 14 incorporates a computer which is linked through the Internet or other communication means to the host database 12. The terminal 14 has a card reader for reading the memory on the card 20, such as a swipe slot, for receiving the card 20 and reading the card identification number from the magnetic strip 26. The terminal 14 also includes a keypad for entering various alphanumeric or other control characters, as well as a display and modem, if necessary, for connection to the host database 12. A plurality of vendor terminals 14 are provided at various outlet locations conveniently situated for customers or users of the system to purchase the cards 20. At the time of purchase, the customer will select one or more of the cards 20 with the desired denominations. The cards 20 are inactive prior to sale and are activated when read by the card reader (FIG. 4). At this time, the terminal 14 conveys information to the host database 12 that the particular card 20 is now active. Effectively, the card 20 is now comparable to a bank note in the hands of a customer. The vendor terminals 14 may conveniently also include unattended kiosk type

automated card dispensers which permit data entry by the customer to select a card denomination value and to insert payment to activate and dispense a card 20. Customers may also obtain the cards 20 from an automated card dispenser that is connected to a communications line to allow the customer to enter data on a keypad provided to correctly enter the required information prior to card activation and dispensing. At the time of purchase, the customer may provide an optional personal identification number which is applied as an extension or addition to the original identification number on the card 20. The same code is then applied to every card 20 that the customer purchases which serves as a further security factor in the use of the cards (as recited in claims 7-8 of the instant application). For example, the customer may be prompted to select a 4-digit number which is entered into the card vendor terminal 14 when the cash card 20 is sold and activated by the magnetic swiping (or other reading device) procedure. In order to use this card, the 4-digit card code must be provided in addition to the card identification number which renders the card 20 usable by the customer only, unless the code is made available to someone else.

The merchant station 16 will typically include an internet website advertising the goods or services for sale. In order to participate in the system 10, the merchant will be registered in the host database 12 and provided with an identification number or other identification means. The merchant is also provided with an account in the host database 12, as well as at a host bank 30, participating in the system 10. Thus, the merchant is able to produce a reference number to identify the goods or services which a particular customer is purchasing, as well as the identification number of the cash

card(s) 20. Although only one merchant station 16 is shown in FIG. 1, there may be a multiplicity of merchants, each with a station 16, registered with the host database 12. The customer may also elect to register with the host database 12 and open a customer account at the host bank 30 which will enable the customer to purchase virtual cash cards over the network, using his or her credit card or other payment means. The virtual cash card is similar to the cash card 20 except that it does not exist physically but is merely represented by its identification number. In this case the system includes a number generator 27 (FIG. 6) for generating a plurality of unique identity numbers associated with different purchasing values. Registration may also enable a customer to accummulate monetary credits when a purchase is made with a card 20 having a value greater than the purchase price of the product or service. In such a case, therefore, instead of forfeiting the difference, the customer's account is credited with the amount. When opening the account, the customer may elect to provide a card code, as referred to above, which will then automatically be applied to any virtual cash card purchased by the customer. The system may also include a host internet website 28 which is in communication with the host database 12 and which is available to customers who are registered with the host database 12 (members) or customers who are not registered (non-members) to browse. This website may also be used by customers, merchants and prospective card vendors to register to participate in the system 10, although card vendors are not necessarily restricted to internet access. Customers who are registered may also be accorded extra privileges and services, such as an account at the host bank 30 with the facility of making deposits and withdrawals in the form of virtual cash

cards, as well as information regarding account balance. The host website may further include directories regarding the goods and services being offered, as well as the registered merchants. Advertising facilities can also be provided for customers or merchants on the website. The host bank 30 may be of a registered federal bank type to which the database 12 has access for effecting the necessary transfers between accounts. A customer will typically have his/her own computer system 18, or other communications equipment, which is connected to the internet and will browse the merchant websites and select goods or services at the merchant websites. For example, the merchant website may include a purchase form which is completed by the customer which makes provision for the entry of the identification number(s) of the card or cards 20 being used for the purchase, as well as for entry of a number or code identifying the goods or services being purchased. These entries are then sent from the merchant station 16 to the host database 12 or processing station connected to the host database 12, where the information is checked and verified, e.g. that the card(s) 20 is active and that the merchant is a recognized registered merchant (FIG. 5). Preferably, the purchase form that is provided to the customer to enter the card identification number is provided only by the host database or website. The merchant website, therefore, provides only a link that directs the customer to the host database or website to avoid the merchant from actually accessing the card identification numbers, for security purposes. If all the entries are complete and verified, the transaction is complete and the host database 12 processes the remainder of the transaction for accounting, billing and tracking. At this time, the merchant is notified of a successful

sale and is prompted to respond according to the type of purchase by notifying the customer of the details of purchase, purchase reference number, delivery date, access code and other details, as desired. At the same time, the host database 12 issues a transaction number to the customer e-mail, if the customer is registered with the host database 112. This transaction number serves as a type of receipt and can also be made available to non-registered customers if they elect to provide the necessary information during the execution of a transaction. If goods are purchased, a goods oriented number is generated which requires that the merchant instantly notifies the customer upon completion of the transaction, via E-mail, of the expected delivery date and a customer contact link for questions and help. If services are purchased, s services type reference number is generated which requires the merchant to notify the customer upon completion, via Email or by other means on the merchant website, details of access to the requested services, such as in the form of a password. After a predetermined minimum period of time, payment is transferred at the host bank 30 from the system account to the merchant account.

The cash cards 20 do not have a declining balance and are designed for one-time use only. According to a further aspect of the invention, any difference between the cash value of a card 20 and the purchase price can be credited to a general account at the host bank which may be used for any designated purpose; eg. as a donation to a host or customer or to a specified charity. Alternatively the difference may be credited to a customer's account at the host bank, as indicated above (see Figures 1-5, col 3 line 10 to col 5 line 30).

Response to Arguments

4. Applicant's arguments filed 2 January 2004 have been fully considered but they are not persuasive.

5. In response to applicant's arguments that Vanstone does not teach the present invention as recited in claims 1-5, examiner respectfully disagrees. As claimed, the prior art of Vanstone does indeed teach the steps of authenticating a client to a server. Although Vanstone may pertain to a situation where a pair of correspondents mutually authenticate each other, the limitations as claimed are met because the client is authenticated to the server. See 35 U.S.C. 102 rejection above. Further, in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the technique of employing only one round trip for authentication, where the authenticity of the server is not in question) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). In addition, in response to applicant's argument that the invention is pertinent to any general transaction, it is respectfully submitted that Vanstone does indeed teach that the secure receipt and transmission of data is performed, hence, these data transactions are pertinent to any general transaction.

In response to applicant's arguments that Fite does not teach the present invention as recited in claims 6-8, examiner respectfully disagrees. It is respectfully submitted that Fite does indeed teach that a one-time use card number is generated at

the user system (see col 3, lines 10-45). Further, the step of activating the card at the issuer system and having the option of adding an extension to the number on the card in Fite is in fact generating the one-time use card number. See 35 U.S.C. 102 rejection above.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ***Lisa M. Caputo*** whose telephone number is **(571) 272-2388**. The examiner can normally be reached between the hours of 8:30AM to 5:00PM Monday through Friday. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached at **(571) 272-2398.** The fax phone number for this Group is (703) 872-9306.

Communications via Internet e-mail regarding this application, other than those under 35 U.S.C. 132 or which otherwise require a signature, may be used by the applicant and should be addressed to [**lisa.caputo@uspto.gov**]. *All Internet e-mail communications will be made of record in the application file. PTO employees do not engage in Internet communications where there exists a possibility that sensitive information could be identified or exchanged unless the record includes a properly signed express waiver of the confidentiality requirements of 35 U.S.C. 122. This is*

more clearly set forth in the Interim Internet Usage Policy published in the Official Gazette of the Patent and Trademark on February 25, 1997 at 1195 OG 89.

LMC
April 17, 2004

DIANE I. LEE
PRIMARY EXAMINER